ASA clientloze SSL VPN-verkeer via IPsec LAN-to-LAN tunnelconfiguratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u verbinding kunt maken met een Cisco adaptieve security applicatie (ASA) clientloze VPN-portal en toegang kunt krijgen tot een server die zich bevindt op een externe locatie en is aangesloten via een IPsec LAN-to-LAN tunnel.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Clientloze SSL VPN-configuratie.
- Configuratie LAN-naar-LAN VPN

Gebruikte componenten

De informatie in dit document is gebaseerd op de ASA 5500-X Series die versie 9.2(1) draait, maar is van toepassing op alle ASA-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Zorg ervoor dat u de mogelijke impact van om het even welke opdracht begrijpt voordat u veranderingen op een levend netwerk aanbrengt.

Achtergrondinformatie

Wanneer een verkeer van een clientloze VPN-sessie een LAN-to-LAN tunnel passeert, moet u opmerken dat er twee verbindingen zijn:

- Van de client naar de ASA
- Van de ASA naar de doelhost.

Voor de ASA-to-bestemming host verbinding wordt het IP-adres van ASA interface "dichtst" bij de doelhost gebruikt. Daarom moet het LAN-to-LAN interessant verkeer een proxy-identiteit uit dat interfaceadres naar het externe netwerk omvatten.

> **Opmerking:** Als Smart-Tunnel voor een favoriet wordt gebruikt, wordt het IP-adres van de ASA interface die het dichtst bij de bestemming ligt nog altijd gebruikt.

Configureren

In dit diagram is er een LAN-to-LAN tunnel tussen twee ASA's die verkeer mogelijk maakt van 192.168.10.x naar 192.168.20.x.

De toegangslijst die interessant verkeer voor die tunnel bepaalt:

ASA 1

```
access-list l2l-list extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0
```

ASA 2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
```

Als de clientloze SSLVPN-gebruiker probeert te communiceren met een host op het 192.168.20.x-netwerk, gebruikt ASA1 het 209.165.200.225-adres als bron voor dat verkeer. Omdat de LAN-to-LAN toegangscontrolelijst (ACL) 209.168.200.225 niet als een proxy-identiteit bevat, wordt het verkeer niet via de LAN-to-LAN tunnel verzonden.

Om verkeer via de LAN-to-LAN tunnel te kunnen verzenden, moet een nieuwe Access Control Entry (ACE) aan het interessante verkeer ACL worden toegevoegd.

ASA 1

```
access-list l2l-list extended permit ip host 209.165.200.225 192.168.20.0
255.255.255.0
```

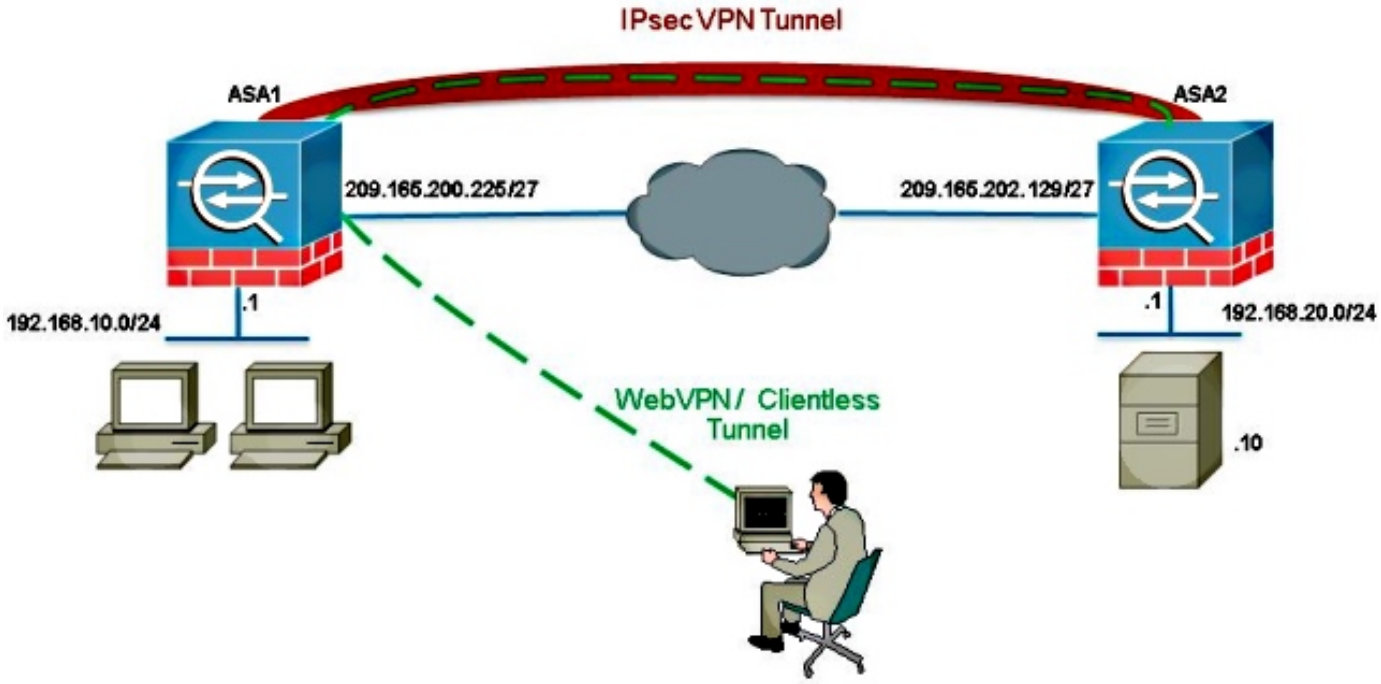
ASA 2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 host
209.165.200.225
```

Dit zelfde beginsel is van toepassing op configuraties waar het clientloze VPN-verkeer dezelfde interface moet **uitschakelen** als deze is ingeschakeld, zelfs indien de client niet via een LAN-naar-LAN tunnel gaat.

> **Opmerking:** Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram



Meestal, ASA2 vertaalt poortadres (PAT) voor de 192.168.20.0/24 om internettoegang te bieden. In dat geval moet het verkeer vanaf 192.168.20.0/24 op ASA 2 worden uitgesloten van het PAT-proces wanneer het naar 209.165.200.225 gaat. Anders gaat de reactie niet door de LAN-to-LAN tunnel. Bijvoorbeeld:

ASA 2

```
nat (inside,outside) source static obj-192.168.20.0 obj-
192.168.20.0 destination
static obj-209.165.200.225 obj-209.165.200.225
!
object network obj-192.168.20.0
nat (inside,outside) dynamic interface
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

- **Laat crypto ipsec sa**-verify met deze opdracht zien dat er een Security Association (SA) tussen het ASA1 Proxy IP-adres en het externe netwerk is gemaakt. Controleer of de versleutelde en gedecrypteerde telers toenemen wanneer de client-SSLVPN-gebruiker die server benadert.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Als de Security Association niet is gebouwd, kunt u IPsec-debugging gebruiken bij de oorzaak van falen:

- **cryptografische beelden reinigen**

  Opmerking: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**